INFORMATION SECURITY

Information security refers to the protection or safeguarding of information and information systems that use, store, and transmit information from unauthorized access, disclosure, alteration, and destruction.

Elements of Information Security

- Confidentiality

Confidentiality is the assurance that the information is accessible only to authorized. Confidentiality breaches may occur due to improper data handling or a hacking attempt.

- Integrity

Integrity is the trustworthiness of data or resources in the prevention of improper and unauthorized changes—the assurance that information is sufficiently accurate for its purpose.

- Availability

Availability is the assurance that the systems responsible for delivering, storing, and processing information are accessible when required by authorized users.

- Authenticity

Authenticity refers to the characteristic of communication, documents, or any data that ensures the quality of being genuine or uncorrupted. The major role of authentication is to confirm that a user is genuine. Controls such as biometrics, smart cards, and digital certificates ensure the authenticity of data

- Non-Repudiation

Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

Motives behind different cyber attacks

- Disrupt business continuity
- Propagate religious or political beliefs
- Perform information theft
- Achieve a state's military objectives
- Manipulating data
- Damage the reputation of the target
- Create fear and chaos by disrupting critical infrastructures
- Take revenge
- Demand ransom
- Bring financial loss to the target

Different kind of Hackers

- A hacker is a person who breaks into a system or network without authorization to destroy, steal sensitive data, or perform malicious attacks. A hacker is an intelligent individual with excellent computer skills, along with the ability to create and explore the computer's software and hardware.
- Black Hats: Black hats are individuals who use their extraordinary computing skills for illegal or malicious purposes. This category of hacker is often involved in criminal activities. They are also known as crackers.
- White Hats: White hats or penetration testers are individuals who use their hacking skills for defensive purposes. These days, almost every organization has security analysts who are knowledgeable about hacking countermeasures, which can secure its network and information systems against malicious attacks. They have permission from the system owner.
- Gray Hats: Gray hats are the individuals who work both offensively and defensively at various times. Gray hats might help hackers to find various vulnerabilities in a system or network and, at the same time, help vendors to improve products (software or hardware) by checking limitations and making them more secure.
- Script Kiddies: Script kiddies are unskilled hackers who compromise systems by running scripts, tools, and software developed by real hackers. They usually focus on the quantity rather than the quality of the attacks that they initiate.
- Insiders: An insider is any employee (trusted person) who has access to critical assets of an organization. An insider threat involves the use of privileged access to violate rules or intentionally cause harm to the organization's information or information systems.

Why Ethical Hacking is necessary

- To prevent hackers from gaining access to the organization's information systems
- To uncover vulnerabilities in systems and explore their potential as a risk
- To analyze and strengthen an organization's security posture, including policies, network protection infrastructure, and end-user practices
- To provide adequate preventive measures in order to avoid security breaches
- To help safeguard the customer data
- To enhance security awareness at all levels in a business

An ethical hacker's evaluation of a client's information system security seeks to answer three basic questions:

1. What can an attacker see on the target system?
2. What can an intruder do with that information?
3. Are the attackers' attempts being noticed on the target systems?

Scope & Limitations of Ethical Hacking

- Gain authorization from the client and have a signed contract giving the tester permission to perform the test.
- Maintain confidentiality when performing the test and follow a Nondisclosure Agreement (NDA) with the client for the confidential information disclosed during the test. The information gathered might contain sensitive information, and the ethical hacker must not disclose any information about the test or the confidential company data to a third party.
- Perform the test up to but not beyond the agreed-upon limits. For example, ethical hackers should perform DoS attacks only if they have previously agreed upon this with the client. Loss of revenue, goodwill, and worse consequences could befall an organization whose servers or applications are unavailable to customers because of the testing.

Skills of Ethical Hacker

- Technical Skills
  - In-depth knowledge of major operating environments, such as Windows, Unix, Linux, and Macintosh
  - In-depth knowledge of networking concepts, technologies, and related hardware and software
  - A computer expert adept at technical domains
  - The knowledge of security areas and related issues
  - High technical knowledge of how to launch sophisticated attacks

- Non-Technical Skills
  - The ability to quickly learn and adapt new technologies
  - A strong work ethic and good problem solving and communication skills
  - Commitment to an organization's security policies
  - An awareness of local standards and laws

Classification of Attacks

Passive Attacks

Passive attacks involve intercepting and monitoring network traffic and data flow on the target network and do not tamper with the data. Attackers perform reconnaissance on network activities using sniffers. These attacks are very difficult to detect as the attacker has no active interaction with the target system or network.

Examples of passive attacks:

Footprinting, Sniffing and eavesdropping, Network traffic analysis, Decryption of weakly encrypted traffic

Active Attacks

Active attacks tamper with the data in transit or disrupt communication or services between the systems to bypass or break into secured systems. Attackers launch attacks on the target system or network by sending traffic actively that can be detected.

Examples of active attacks:

Denial-of-service (DoS) attack, Firewall and IDS attack, Bypassing protection mechanisms, Malware attacks (such as o Arbitrary code execution, viruses, worms, ransomware) Privilege escalation etc.

Classification of Attacks

Close-in Attacks

Close-in attacks are performed when the attacker is in close physical proximity with the target system or network. The main goal of performing this type of attack is to gather or modify information or disrupt its access. For example, an attacker might shoulder surf user credentials. Attackers gain close proximity through surreptitious entry, open access, or both.

Examples of close-in attacks:

Social engineering (Eavesdropping, shoulder surfing, dumpster diving, and other methods)

Insider Attacks

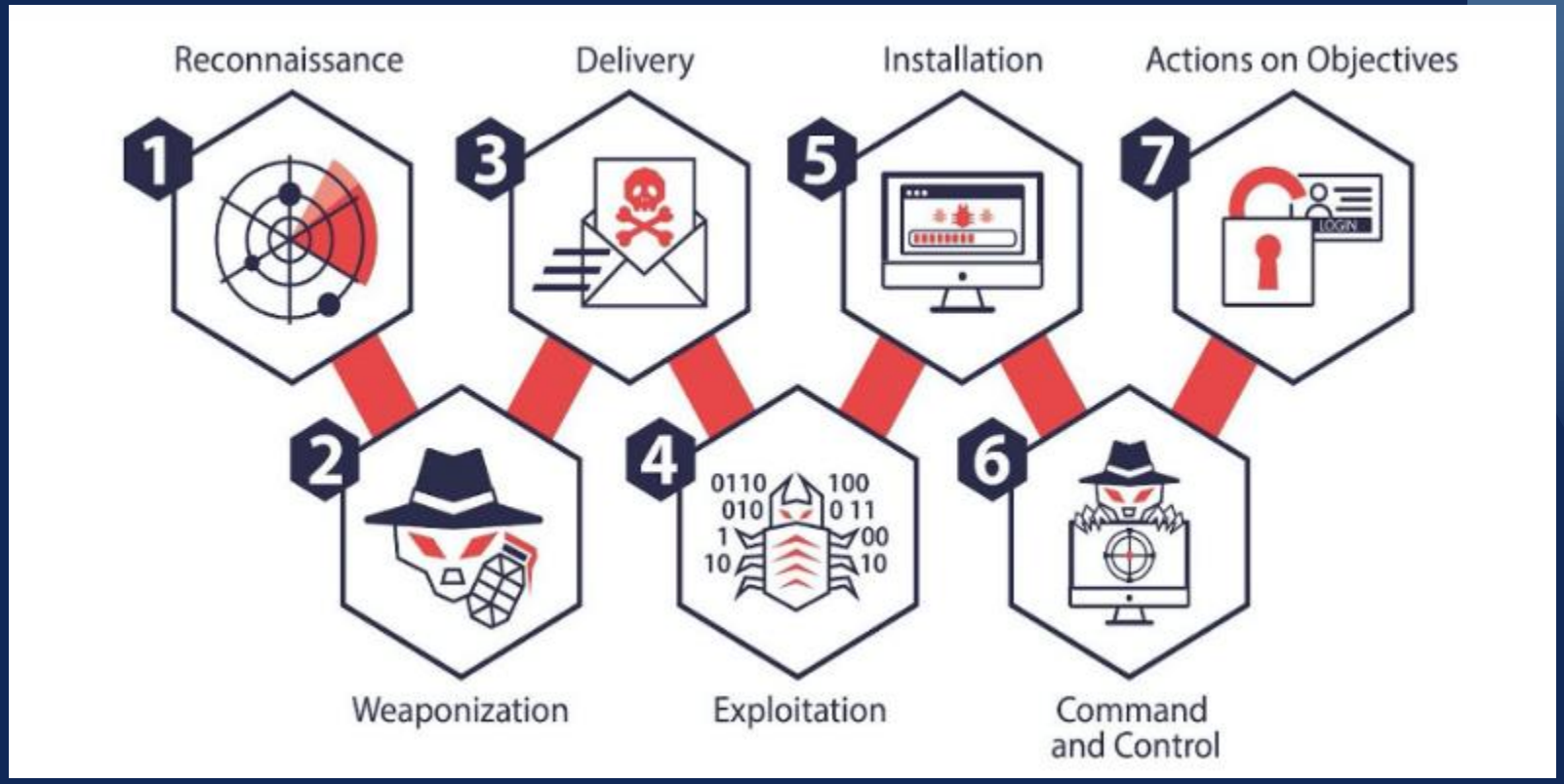
Insider attacks are performed by trusted persons who have physical access to the critical assets of the target. An insider attack involves using privileged access to violate rules or intentionally cause a threat to the organization's information or information systems.

Examples of insider attacks:

Eavesdropping and wiretapping, Theft of physical devices, Social engineering etc.

Cyber Kill Methodology

The cyber kill chain methodology is a component of intelligence-driven defense for the identification and prevention of malicious intrusion activities. This methodology helps security professionals in identifying the steps that adversaries follow in order to accomplish their goals. The cyber kill chain is a framework developed for securing cyberspace based on the concept of military kill chains. This method aims to actively enhance intrusion detection and response. The cyber kill chain is equipped with a seven-phase protection mechanism to mitigate and reduce cyber threats.



Tactics, Techniques & Procedures

One security framework, MITRE ATT&CK, is a comprehensive collection of TTPs that attackers use in the real world. Let's define each part of the TTP triangle:

- **Tactics:** The high-level description of the behavior and strategy of a threat actor. The tactic includes a set of behaviors and actions employed by the adversary to achieve a specific objective.
- **Techniques:** These are the non-specific guidelines and intermediate methods that describe how a tactic action can be realized.
- **Procedures:** These refer to the sequence of actions performed using a technique to execute on an attack tactic. The procedure involves detailed descriptions on the tailored activities that enable a threat actor to successfully achieve their targets.

Risk Management

- Risk refers to the degree of uncertainty or expectation of potential damage that an adverse event may cause to the system or its resources, under specified conditions. Alternatively, risk can also be:
  - The probability of the occurrence of a threat or an event that will damage, cause loss to, or have other negative impacts on the organization, either from internal or external liabilities.
  - The possibility of a threat acting upon an internal or external vulnerability and causing harm to a resource.
  - The product of the likelihood that an event will occur and the impact that the event might have on an information technology asset.
- The relation between Risk, Threats, Vulnerabilities, and Impact is as follows:

  RISK = Threats x Vulnerabilities x Impact
- The impact of an event on an information asset is the product of vulnerability in the asset and the asset's value to its stakeholders. IT risk can be expanded to

  RISK = Threat x Vulnerability x Asset Value

- Risk management is the process of identifying, assessing, responding to, and implementing the activities that control how the organization manages the potential effects of risk.

Risk Management Phases

The four key steps commonly termed as risk management phases are:

- Risk Identification
- Risk Assessment
- Risk Treatment
- Risk Tracking and Review

Cyber security Compliance Standards

1. HIPAA (Health Insurance Portability and Accountability Act):
    1. **Region**: United States
    2. **Focus**: Protecting the privacy and security of patients' health information.
2. GDPR (General Data Protection Regulation):
    1. **Region**: European Union (applies globally for organizations handling EU residents' data).
    2. **Focus**: Safeguarding personal data and prioritizing individual privacy rights.
3. PCI DSS (Payment Card Industry Data Security Standard):
    1. **Region**: Worldwide
    2. **Focus**: Securing payment card data.
4. ISO 27001:
    1. **Region**: Worldwide
    2. **Focus**: Comprehensive framework for managing information security.
5. SOC 2 (Service Organization Control 2):
    1. **Region**: United States
    2. **Focus**: Security, availability, processing integrity, confidentiality, and privacy of customer data.